Eventlog to Syslog v4.5

Release 4.5
Last revised September 29, 2013

This product includes software developed by Purdue University.

The Eventlog to Syslog utility is a windows service originally created by Curtis Smith at Purdue University. The original utility and source code can be found at the following website: https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys/

Version 4 was modified by Sherwin Faria in July, 2009, in order to meet the needs of Rochester Institute of Technology.

This update of the Eventlog to Syslog client builds upon the original code by offering several bug fixes and some additional features.

Changes in v4.5:

- Addition of a Tag (-t) parameter allowing you to specify a custom parameter for the program field.
- Addition of a parameter (-a) allowing use of an FQDN Hostname or IP address
- IncludeOnly flag no longer used on Vista/Server 2k8
- Allow use of XPath to specify events to forward on Vista/2008+
- Removal of additional DLL, now a single file deployment
- Removal of additional log host keys switching to instead use a single key

Changes in v4.4.1:

- Fixed a bug checking the windows events engine installed

Send all comments, questions, bug reports, and requests to:

Sherwin Faria
sherwin.faria@gmail.com

TABLE OF CONTENTS

1. Usage:

```
Version: 4.4 (32-bit)
Usage: evtsys -i|-u|-d [-h host[;host2;...]] [-f facility] [-p port]
       [-t tag] [-s minutes] [-q bool] [-l level] [-n] [-a]
  -i           Install service
  -u           Uninstall service
  -d           Debug: run as console program
  -a           Use our IP address (or fqdn) in the syslog message
  -h host      Name of log host(s), separated by a ';'
  -f facility  Facility level of syslog message
  -l level     Minimum level to send to syslog.\n", stderr);
               0=All/Verbose, 1=Critical, 2=Error, 3=Warning, 4=Info
  -n           (**Win9x/Server 2003 Only**) Include only those events specified
               in the config file.
  -t tag       Include tag as program field in syslog message
  -p port      Port number of syslogd
  -q bool      Query the Dhcp server to obtain the syslog/port to log to
               (0/1 = disable/enable)
  -s minutes   Optional interval between status messages. 0 = Disabled

Default port: 514
Default facility: daemon
Default status interval: 0
Host (-h) required if installing.
```

2. Installing the Service

The Service installs eight registry values in **HKLM\SOFTWARE\ECN\EvtSys\3.0**

Facility	(DWORD)	Default: 3
IncludeOnly	(DWORD)	Default: 0
LogHost	(String)	Default: N/A
LogHost2	(String)	Default: <empty>
LogLevel	(DWORD)	Default: 0
Port	(DWORD)	Default: 514
QueryDhcp	(DWORD)	Default: 0
StatusInterval	(DWORD)	Default: 0

If no secondary host is specified LogHost2 is blank.
It also registers itself as a service under the name evtsys and displays in services.msc as “Eventlog to Syslog”.

The program must be installed from the command line
After you have run evtsys.exe with the *-i* switch and specified a loghost you can then type *net start evtsys* to start the service.
To start or stop the service from the command line type: ***net start evtsys*** or ***net stop evtsys***
Alternatively you can start the service from the Services control panel in Administrative Tools. Look for "Eventlog to Syslog".

2.1. Using a DHCP Option

The DHCP option is called *EventToSyslogDhcpOption*. It is in the format x.x.x.x

Notes: (Courtesy of Damien)
Microsoft Windows has a big problem with non-standard DHCP options which need us to "install" a "persistent DHCP request" in order to be able to retrieve it...

I have seen some windows still not being able to get us the standard options without using a persistent request, so activating this branch of code will do the trick, just notice that in order to work, the system will only work after the second boot, because as said in MSDN docs, the persistent request is only done at boot time, so the first registers the request, the second boot does it.

In the sake of being completely documented, knowing where to look in case things go wrong:

HKLM\System\CurrentControlSet\Services\Dhcp\Parameters:
the GUID keys are the GUID of the network adapters, and the values are simply the DHCP packets, so look into those values, and you will read the options as passed by the DHCP server (you will recognize the options windows say it knows nothing about.. but here they are).

HKLM\System\CurrentControlSet\Services\Dhcp\Parameters\Options:
lists the "options" windows know about, kind of factory defaults. Unusable for us, but it is here that you will see new keys appear when you activate the "persistent request" mechanism.

2.2. Using FQDN

When using the –a switch, the service will attempt to lookup the FQDN of the local machine. If successful it will send the FQDN in the syslog message as the host. If unsuccessful it will use the machines IP address.

2.3. Specifying a Tag

Specify a tag with the –t switch and the tag will be specified in the program field of each syslog message.

2.4. Removal of additional DLL file

The need for a separate DLL file has been removed. It’s sole purpose was to specify message keys for log messages. The keys have now been built into the executable during compilation. The reference to the DLL in
HKLM\System\CurrentControlSet\Services\EventLog\Application\EvtSys\EventMessageFile

should be automatically updated to the exe on first run. If you notice errors in the log about missing message keys from evtsys, check that value.

3. Uninstalling

Uninstalling the service will delete the registry keys created during installation and unregister the Eventlog to Syslog service. All files will remain in their current location.

Note: Some users have reported not being able to completely remove the service while the Services control panel is open. I have not been able to reproduce this issue, but it is something to be aware of.

4. Debug Mode

Debug mode provides additional information on the operation of the service.
The following information is displayed while in debug mode:

- The source and ID of an ignored event
- All error messages

5. Specifying Log Hosts

Use the command line switch *–h* o specify your primary and any secondary Syslog servers. Multiple syslog servers are separated by a semicolon ';'. The *–h* is required when installing the agent.

You may specify either the hostname or IP address of a host. The utility will convert the hostname into an IP address and store that address into the registry.

6. Specifying Facility

The Syslog protocol specifies 24 facilities:

0 kernel messages
1 user-level messages
2 mail system
3 system daemons
4 security/authorization messages
5 messages generated internally by syslogd
6 line printer subsystem
7 network news subsystem
8 UUCP subsystem
9 clock daemon
10 security/authorization messages
11 FTP daemon
12 NTP subsystem
13 log audit
14 log alert
15 clock daemon
16 local use 0 (local0)
17 local use 1 (local1)
18 local use 2 (local2)

19 local use 3 (local3)
20 local use 4 (local4)
21 local use 5 (local5)
22 local use 6 (local6)
23 local use 7 (local7)

By default the “Eventlog to Syslog” service logs to facility 3, system daemon, but it can be configured to log to whatever facility you specify using the *–f* switch.

7. Appendix

7.1. The Configuration File

If no configuration file is found a default configuration file is generated with the following contents:

```
'!!!!THIS FILE IS REQUIRED FOR THE SERVICE TO FUNCTION!!!!
'
'Comments must start with an apostrophe and
'must be the only thing on that line.
'
'Do not combine comments and definitions on the same line!
'
'Format is as follows - EventSource:EventID
'Use * as a wildcard to ignore all ID's from a given source
'E.g. Security-Auditing:*
'
'In Vista/2k8 and upwards remove the 'Microsoft-Windows-' prefix
'In Vista/2k8+ you may also specify custom XPath queries
'Format is the word 'XPath' followed by a ':', the event log to search,
'followed by a ':', and then the select expression
'E.g XPath:Application:<expression>
'
'Details can be found in the readme file at the following location:
'https://code.google.com/p/eventlog-to-syslog/downloads/list
'**********************:**************************
XPath:Application:<Select Path="Application">*</Select>
XPath:Security:<Select Path="Security">*</Select>
XPath:Setup:<Select Path="Setup">*</Select>
XPath:System:<Select Path="System">*</Select>
```

7.2. Specifying XPath Queries

On Vista/Server 2008 and beyond Evtsys uses XPath queries to subscribe for events. It uses the same filter format you find in the new Event Viewer when you create a custom view.

The format is as follows:
`XPath:<PathtoChannel>:<Select statement>`

Currently it must reside on one line. Making that more user friendly may be a future enhancement. All you will need is the `<Select...>` statements, don't worry about the `<Query>` or `<QueryList>` tags.

Event Viewer Examples:

```
<Query Id="0" Path="Security">
  <Select Path="Security">*[System[Provider[@Name='Microsoft-Windows-
Eventlog' or @Name='EvtSys'] and (EventID=1301 or EventID=1302)]]</Select>
```

```
</Query>

<QueryList>
  <Query Id="0" Path="Microsoft-Windows-Dhcp-Client/Admin">
    <Select Path="Microsoft-Windows-Dhcp-Client/Admin">*</Select>
    <Select Path="Microsoft-Windows-Dhcp-Client/Operational">*</Select>
  </Query>
</QueryList>
```

Config File Examples:

```
XPath:Application:<Select Path="Application">*</Select>
'XPath:Security:<Select Path="Security">*</Select>
XPath:Setup:<Select Path="Setup">*</Select>
XPath:System:<Select Path="System">*</Select>
XPath:Microsoft-Windows-Dhcp-Client/Admin:<Select Path="Microsoft-Windows-
Dhcp-Client/Admin">*</Select>
XPath:Security: <Select
Path="Security">*[System[Provider[@Name='Microsoft-Windows-Eventlog' or
@Name='EvtSys'] and (EventID=1301 or EventID=1302)]]</Select>
```

If you delete your config file it will generate a new one with additional comments and some default filters. The IncludeOnly flag no longer has any effect on Server 2008+. You will now only receive events you have specified in the config file on Vista/2008+. Older versions of Windows will function as they did previously.

You can use the same config file for both older and newer version of Windows Server as the utility will ignore the XPath config option on older versions.

7.3. The Status File (Obsolete)

The status file is updated by the agent approximately every two minutes. The agent places a single line in the file in the following format:
Mmm dd hh:mm:ss - Eventlog to Syslog Service Running
You may delete this file at any time and the agent will recreate it at the next interval.

7.4. Minimum Log Level/Severity

The LogLevel registry key limits the events that are processed by the utility. Only logs with a severity less than or equal to the set level will be processed. The severity ratings are as follows:

Type	**Pre-2k8**	**Vista/2k8+**
CRITICAL	N/A	1
ERROR	1 or 2	2
WARNING	3	3
INFO	4	4
AUDIT/ALL	0	0

Note: Since a CRITICAL severity is not available on systems prior to Vista/2k8, Level 1 is mapped to error, which is 2.

7.5. The IncludeOnly Flag

By setting the include only flag you cause the service to treat the contents of the configuration file as allowed events. Any events NOT specified in the file will be ignored.

When the flag is false, any events that ARE specified in the file are ignored.

Note: This flag is only used Pre-Vista/Server 2008. With Server 2008 and beyond it is always IncludeOnly and you must specify any events you want sent.

7.6. Miscellaneous

7.6.1. Maximum message size

The maximum size of a Syslog message is defined as 1024 bytes. Anything beyond this threshold is truncated. The LP (Large Packet) version has a maximum size of 4096 bytes.

7.6.2. Polling interval

The "Eventlog to Syslog" service polls for messages every 5 seconds on Pre-2008 boxes. On Server 2008+ it uses a subscriber/consumer model.

7.6.3. Timestamps

Event timestamps are captured from the event itself.
The agent generates its own timestamps for error and informational messages.

7.7. Compiling

Compiling the service requires Microsoft Visual Studio. I use 2010, but earlier versions should also work.

You can change the type of compile you are doing using the vcvarsall.bat script. Details can be found at this site: http://msdn.microsoft.com/en-us/library/x4d2c09s(VS.80).aspx

1. Open the appropriate Visual Studio Command Prompt in (There may be 32Bit and 64Bit shortcuts)Start>Programs>Visual Studio 200x>Visual Studio Tools
2. Navigate to the directory containing the source files
3. Type `nmake`
4. Wait for the task to complete. All you will need is evtsys.exe and evtsys.dll. There is also an evtsys.pdb file created for debugging if you choose to keep it.
5. Once completed you can type `nmake clean` to delete all created files, but be sure to move evtsys.exe and evtsys.dll first as those will also be deleted.

8. Changelog

Changes in v4.4.3:

- Improved performance in Server 2008 by implementing event subscriptions. Thanks to Martin for pointing me in the right direction.

Changes in v4.4.2:

- Added support for custom tags from a server. Use the -t flag when installing (Thanks wired)
- Added support for up to four log hosts simultaneously
- Fix a bug that causes excessive errors when an event cannot be retrieved on Server 2008
- Fix an issue not allowing a log level of 4 to be valid
- Began support for configurable maximum log size. Not yet completed
- Lightly tested TCP support has been implemented. Error checking and fault tolerance not yet finished. Documentation will be forthcoming for those who want to help test it

Changes in v4.4.1:

- Fixed a bug checking the windows events engine installed

Changes in v4.4:

- Finally added the ability to send only specified events
- Set Audit Failures to show as Error instead of Notice on Vista/2k8+
- Allow user to specify the minimum severity to process
- Added registry keys to configure the minimum severity and modeThe keys are LogLevel and IncludeOnly. Both DWORD values where 0 is disabled. See readme for additional details.

Changes in v4.3.1:

- Bugfix: Fixed bug where hostnames on Server 2003 and earlier were getting an extra leading space.

Changes in v4.3:

- Fixed a crash dealing with ignored events (Thanks to Pavel)
- Wildcards now work in the config file for event IDs. So to ignore all events from a given source, the format would be: SourceName:*
- Got rid of the evtsys.stat file. Sends the message to the Syslog server instead
- Added a registry key to control if and when the status message is sent.The key is called StatusInterval with type DWORD and you specify a time in minutes. 0 means disabled.

Changes in v4.2:

- Thanks to Damien Mascre for his help with this update (UTF-8 and DHCP)
- Added UTF-8 support, so messages are now sent using UTF-8 encoding
  Note: Tested using Syslog Watch Personal. Had to force UTF-8 codepage
- Added hostname immediately after timestamp to comply with RFC-3164
- Added ability to use a DHCP option to set syslog server (by Damien)
- Removed spaces from event source (tag) field in sent message

Changes in v4.0:

- Added ability to ignore specific events
- Added a status file for monitoring service operation
- Added event’s timestamp to outgoing messages
- Added compatibility with the Vista/Server 2008 Windows Events service
- Added ability to send to two Syslog servers simultaneously
- Fixed a possible memory exception with bad message definitions
- Fixed a bug where utility would not search all message files

7.8 FAQ

Q: I am using syslog-ng and no logs are showing up on my syslog server, what gives?
A: Try making sure your host filters in syslog-ng are uppercase. Syslog-ng hostname matching is case sensitive